Claim Amendments

Claim 1 (currently amended): A secure telecommunications system comprising:

[[a]] an external network on which traffic travels;

a switch connected to the external network;

an internal network connected to the switch;

a first inspection engine connected to the switch and not in line with the internal network and the external network, which receives traffic from the switch, processes the traffic to determine whether it is desired traffic or undesired traffic, which prevents undesired traffic from passing through it and which sends desired traffic back to the switch;

a second inspection engine connected to the switch and not in line with the internal network and the external network, which receives traffic from the switch, processes the traffic to determine whether it is desired traffic or undesired traffic, which prevents undesired traffic from passing through it and which sends desired traffic back to the switch;

-2-

a first destination connected to the switch through the internal network which

receives desired traffic from the switch that has been processed by the first inspection engine;

and

a second destination connected to the switch through the internal network which

receives desired traffic from the switch that has been processed by the second inspection

engine.

Claim 2 (original): A system as described in Claim 1 wherein the first

inspection engine includes a first firewall processing engine and the second inspection engine

includes a second firewall processing engine.

Claim 3 (currently amended): A system as described in Claim 2 wherein the

switch has a first port and a second port connected to the external network which receives

traffic from the external network, said switch directing traffic received at the first port to the

first firewall processing engine and directing traffic received at the second port to the second

firewall processing engine.

Claim 4 (original): A system as described in Claim 3 including N additional

firewall processing engines connected to the switch besides the first firewall processing engine

and the second firewall processing engine so there are a total of N+2 firewall processing engines, where N is greater than or equal to 1 and is an integer.

Claim 5 (original): A system as described in Claim 4 wherein the switch has N additional ports besides the first port and the second port, wherein each port is connected to a corresponding firewall processing engine.

Claim 6 (original): A system as described in Claim 5 wherein the switch is configured into security groups with at least one of the N+2 firewall processing engines serving each security group.

Claim 7 (original): A system as described in Claim 6 wherein the switch load-shares traffic for each security group across corresponding firewall processing engines serving the corresponding security group.

Claim 8 (original): A system as described in Claim 7 wherein the switch rebalances traffic for a security group when one of the firewall processing engines serving the security group fails across the other firewall processing engines serving the security group.

Claim 9 (original): A system as described in Claim 8 wherein the switch is scalable to allow for adding firewall processing engines.

Claim 10 (original): A system as described in Claim 9 wherein the traffic includes bits and wherein the firewall processing engines serving a first security group of the security groups encrypt greater than 1 Gbps of traffic.

Claim 11 (currently amended): A system as described in Claim 10 wherein the external network includes the Internet, and the first destination includes a first web server and the second destination includes a second web server.

Claim 12 (original): A system as described in Claim 11 wherein the Internet includes a LAN.

Claim 13 (currently amended): A method for sending traffic over a secure telecommunications system comprising the steps of:

receiving traffic from [[a]] an external network at a switch connected to the external network and an internal network;

directing traffic to a first inspection engine connected to the switch and not in line with the internal network or the external network, and to a second inspection engine connected to the switch and not in line with the internal network or the external network;

receiving traffic at the first inspection engine;

processing traffic received at the first inspection engine to determine whether it is desired traffic or undesired traffic;

sending the desired traffic back to the switch from the first inspection engine and discarding undesired traffic from the first inspection engine;

transferring desired traffic received by the switch from the first inspection engine to a first destination through the internal network;

processing traffic received at the second inspection engine to determine whether it is desired traffic or undesired traffic;

sending the desired traffic back to the switch from the second inspection engine and discarding undesired traffic from the second inspection engine; and

transferring desired traffic received by the switch from the second inspection engine to a second destination through the internal network.

Claim 14 (original): A method as described in Claim 13 wherein the first and second inspection engines include a first firewall processing engine and a second firewall processing engine, respectively, and wherein the directing traffic step includes the step of directing traffic to the first firewall processing engine and second firewall processing engine and to a third firewall processing engine and a forth firewall processing engine.

Claim 15 (original): A method as described in Claim 14 wherein the switch is configured into a first security group and a second security group, and the receiving step includes the step of receiving traffic at the first security group.

Claim 16 (original): A method as described in Claim 15 wherein the directing step includes the step of directing the traffic from the first security group of the switch to the first, third and fourth firewall processing engines which serve the first security group of the switch, and directing traffic to the second firewall processing engine serving the second security group of the switch.

Claim 17 (original): A method as described in Claim 16 wherein the receiving step includes the step of receiving traffic from the first security group at a first port of the switch and receiving traffic for the second security group at a second port of the switch.

Claim 18 (original): A method as described in Claim 17 wherein the directing the traffic from the first security group includes the step of load-sharing by the switch the traffic received by the first security group between the first, third and fourth firewall processing engines.

Claim 19 (original): A method as described in Claim 18 wherein the directing the traffic from the first security group includes the step of rebalancing traffic from the first security group to the third and fourth firewall processing engines when the first firewall processing engine fails.

Claim 20 (original): A method as described in Claim 19 wherein after the step of transferring traffic to the first destination, there is the step of connecting a fifth firewall processing engine to the switch.